Exhibit 87

Login

Watch TV

FEATURES · **Published** October 29, 2018

Security-challenged firms are gatekeepers of US elections

By FRANK BAJAK | **Associated Press**

Image 1 of 2

In this July 11, 2018, photo, Peter Lichtenheld, vice president of operations for voting systems vendor Hart InterCivic, testifies during a Senate hearing on election security in Washington. Experts say top election vendors have long skimped on security in favor of convenience and use proprietary systems, making it more difficult to detect election meddling. (AP Photo/Cliff Owen)

The ultimate gatekeepers of U.S. election integrity may well be its weakest security link.

A trio of privately held companies sells and services more than 90 percent of U.S. elections systems. But the companies have long stressed convenience for its customers over product security, security experts and elections officials said.

That complicates efforts to detect a repeat of Russia's 2016 election meddling, or other intrusions by sophisticated hackers.

The three companies — ES&S of Omaha, Nebraska; Dominion Voting Systems of Denver and Hart InterCivic of Austin, Texas — face little public accountability and operate under a shroud of financial and operational secrecy despite their pivotal role underpinning American democracy.

They face scant federal oversight yet effectively run elections, directly or through subcontractors, in much of the nation — especially where tech expertise and budgets are thin. No federal authority accredits the vendors or vets them.

High barriers to entry and low profits discourage the very innovations that could enhance security, experts say.

"They cobble things together as well as they can" because building truly secure systems would likely erase their profits, said University of Connecticut election-technology expert Alexander Schwartzman.

Executives of all three of the top vendors refused to discuss their companies' finances and have resisted exposing their products to the scrutiny of independent researchers and Congress.

"These companies want to be gatekeepers of our democracy but they seem completely uninterested in safeguarding it," Sen. Ron Wyden, an Oregon Democrat, complained in a July congressional hearing.

The top three vendors call such concerns overblown, and say there is no indication hackers have penetrated any of their systems.

But authorities say serious election mischief may have gone unnoticed, and hackers could theoretically wreak havoc at multiple stages of the election process. They could alter or erase lists of registered voters to sow confusion, secretly introduce software to flip votes, scramble tabulation systems or knock results-reporting sites offline with denial-of-service attacks.

On July 13, U.S. special counsel Robert Mueller indicted 12 Russian military intelligence operatives for, among other things, infiltrating state and local election systems.

Election vendors have long resisted open-ended vulnerability testing by independent, ethical hackers — a process that aims to identify weaknesses an adversary could exploit. Such testing is now standard for the Pentagon and major banks.

Nevertheless, the vendors insist security is a priority. ES&S, for instance, said in an email that "any assertions about resistance to input on security are simply untrue" and argued that for decades the company has "been successful in protecting the voting process."

Experts point to numerous indications of sloppy software development and unfixed vulnerabilities.

"The industry continues to stonewall the problem," said Bruce McConnell, a Department of Homeland cybersecurity czar during the Obama administration. Election-vendor executives issue bland assurances but don't, for instance, offer "bug bounties" to researchers who look for software flaws, he said.

In July, ES&S told The Associated Press that it allows independent, open-ended testing of its corporate systems as well as its products. But the company would not name the testers and declined to provide documentation of the testing or its results.

Dominion's vice president of government affairs, Kay Stimson, said her company has also had independent third parties probe its systems but would not name them or share details.

Hart InterCivic, the No. 3 vendor, said it has done the same using the Canadian cybersecurity firm Bulletproof, but would not discuss the results.

ES&S hired its first chief information security officer in April. None of the big three would say how many cybersecurity experts they employ. Dominion's Stimson said "employee confidentiality and security protections outweigh any potential disclosure."

During this year's primary elections, ES&S technology stumbled on several fronts.

In Los Angeles County, more than 118,000 names were left off printed voter rolls. A subsequent outside audit blamed sloppy system integration by an ES&S subsidiary during a database merge.

No such audit was done in Kansas' most populous county after a different sort of error in newly installed ES&S systems delayed the vote count by 13 hours as data uploading from thumb drives crawled.

University of Iowa computer scientist Douglas Jones said both incidents reveal mediocre programming and insufficient pre-election testing. And voting equipment vendors have never seemed security conscious "in any phase of their design," he said.

California, New York and Colorado are among states that tend to keep a close eye on the vendors. States with cozier relationships have in the past let them use remote-access software to do maintenance on election systems, a widely discredited security faux pas.

And ES&S continues to sell vote-tabulation systems equipped with cellular modems, a feature experts say hackers could potentially exploit, entering election management modules and tamper with vote counts.

A few states ban such wireless connections. Maryland recently got rid of them and Alabama forced ES&S in January to remove them from machines.

Said John Bennett, the Alabama secretary of state's deputy chief of staff who worked the issue: "It seemed like there was a lot more emphasis about how cool the machines could be than there was actual evidence that they were secure."

___

Frank Bajak on Twitter: https://twitter.com/fbajak